IN THE CLAIMS:

1. (Currently Amended) A method, comprising:

generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet and algorithm initialization information, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained, where [[and]] no pre-established security association is needed to verify the packet;

generating a packet header, comprising the validity information, ~~and comprising generating the algorithm information which comprises values to initialize an algorithm to be used to perform the validity check of the packet~~; and

sending the packet including the packet header from a first network node to a second network node.

2. (Previously Presented) The method according to claim 1, wherein the generating of the validity information comprises generating security information indicating security services applied to the packet.

3. (Cancelled)

4. (Previously Presented) The method according to claim 1, wherein the generating of the algorithm information comprises generating the algorithm information which indicates an algorithm to be used to perform the validity check of the packet.

5.-10. (Cancelled).

11. (Currently Amended) The method according to claim [[6]] 1, wherein the generating of the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

12. (Previously Presented) The method according to claim 1, wherein the generating of the validity information comprises generating an information item to prevent replay attacks.

13. (Previously Presented) The method according to claim 12, wherein the generating of the information item comprises including in the information item an indication of a procedure to be used for anti replay attacks.

14. (Previously Presented) The method according to claim 12, wherein the generating of the information item comprises including in the information item a time stamp.

15. (Currently Amended) The method according to claim [[6]] 1, further comprising:

signing the packet using a private key corresponding to [[a]] the public key indicated by the validity information ~~in the packet header in a sending network node~~.

16-17. (Cancelled)

18. (Currently Amended) An apparatus, comprising:

validity information generating means for generating validity information for a packet;

packet header generating means for generating a header for the packet, comprising the validity information; and

sending means for sending the packet including the header to a receiving network node,

wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises

algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

19.-41. (Cancelled)

42. (Currently Amended) An apparatus, comprising:

a validity information generator configured to generate validity information for a packet;

a packet header generator configured to generate a header for the packet, comprising the validity information; and

a transmitter configured to send the packet including the header to a receiving network node,

wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key

information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

43. (Previously Presented) The apparatus according to claim 42, wherein the validity information comprises security information indicating security services applied to the packet.

44.-49. (Cancelled)

50. (Currently Amended) The apparatus according to claim [[45]] 42, wherein the public key information comprises public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

51. (Previously Presented) The apparatus according to claim 42, wherein the validity information comprises an information item to prevent replay attacks.

52. (Previously Presented) The apparatus according to claim 51, wherein the information item to prevent replay attacks contains an indication of a procedure to be used for anti-replay attacks.

53. (Previously Presented) The apparatus according to claim 51, wherein the information item to prevent replay attacks contains a time stamp.

54. (Previously Presented) The apparatus according to claim 42, further comprising:

a signor configured to sign the packet using a private key corresponding to a public key indicated by the validity information in the packet header in the sending network node.

55. (Currently Amended) An apparatus, comprising:

a receiver configured to receive packets from a sending network node; and

a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required to perform the validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

56. (Previously Presented) The apparatus according to claim 55, wherein the validity information comprises security information indicating security services applied to the packet.

57.-58. (Cancelled)

59. (Currently Amended) An apparatus, comprising:

a transmitter configured to forward packets from a sending network node to a receiving network node; and

a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

60. (Previously Presented) The apparatus according to claim 59, wherein the validity information comprises security information indicating security services applied to the packet.

61. Cancelled.

63. (Currently Amended) A method, comprising:

receiving packets at a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

64. (Currently Amended) A method, comprising:

forwarding received packets to a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

65. (Cancelled)

66. (Currently Amended) A computer program configured to operate on a computer readable storage medium, that when executed controls a processor to perform:

generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used to perform the validity

check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained;

generating a packet header, comprising the validity information; and

sending the packet including the header from a first network node to a second network node.

67. (Currently Amended) A computer program configured to operate on a computer readable storage medium, that when executed controls a processor to perform:

receiving packets at a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key

information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.

68. (Currently Amended) A computer program configured to operate on a computer readable storage medium, that when executed controls a processor to perform:

forwarding received packets to a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising one of the public key of the sending node or an identity of an entity from which the public key of the sending node can be obtained.